IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Gordon GOOD	§	Confirmation No.:	4076
Serial No.:	09/852,244	§	Group Art Unit:	2437
Filed:	May 10, 2001	§	Examiner:	Paul E. Callahan
For:	Security Policy Management For Network Devices	§	Docket No.:	200704491-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: March 23, 2011

Sir:

Appellant hereby submits this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on January 26, 2011.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, Texas, 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC. An Assignment to HPDC was recorded on May 7, 2008, at Reel/Frame 0209090707.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-13.
Claim cancellations:	14, 15, 18, 19, 23, and 32.
Added claims:	14-42.
Presently pending claims:	1-13, 16-17, 20-22, 24-31, and 33-42.
Presently allowed claims:	None.
Presently appealed claims:	1-13, 16-17, 20-22, 24-31, and 33-42.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the final Office action dated October 27, 2010.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellant. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

To support an entity's website operations, a website requires an infrastructure that stores the information provided by that site, responds to user requests for the information, and conducts other types of transactions appropriate to the site.[1] While an entity may create and support its own "website," some entities may desire to have their websites supported by an organization that specializes in such a service, such as a managed service provider.[2] In such a situation, employees of the various entities may require access to the servers and other devices that support their respective websites, for example to update content, perform routine maintenance, etc.[3] At the same time, personnel at the support organization also require access to these devices, to upgrade, reconfigure or retire components of the infrastructure.[4] When a single organization is responsible for supporting the data of multiple entities, and different groups of people require access to that data, a problem

[1] P. 1, lines 21-24.

[2] P. 2, lines 11-13.

[3] P. 2, lines 13-16.

[4] P. 2, lines 16-18.

may arise in supporting the individual needs of each of the various entities.[5] For example, each of the respective entities can have specific policies or procedures with regard to their respective information.[6] For example, security polices may be established which define who has permission to access what information.[7] Such a security policy can establish that a particular individual has the authority to access all devices associated with a particular entity, whereas other individuals such as developers may only be authorized to access a subset of the devices associated with the entity.[8]

A common solution involves manually configuring each device.[9] For example, each device may be configured with access lists or user-password pairs that identify who has access to the device.[10] This solution, while providing some data security, has its limitations.[11] For example, when the system requires updating, it can be difficult to find all of the instances of, for example, the user-password pairs, leaving the system vulnerable to unauthorized access.[12] Furthermore, the infrastructure required to support large websites may include numerous computing devices, such as web servers, database servers, and application servers, requiring significant maintenance effort.[13]

Appellant has devised techniques for implementing security policy by means of machine-readable descriptions (*i.e.*, account templates).[14] The templates represent policies applicable to all of the computing devices within a

---

[5] P. 2, lines 18-21.

[6] P. 2, lines 21-22.

[7] P. 2, lines 22-24.

[8] P. 2, lines 24-27.

[9] P. 2, lines 28-29.

[10] P. 2, line 29 to P. 3, line 1.

[11] P. 3, lines 1-2.

[12] P. 3, lines 2-5.

[13] P. 3, lines 5-8.

[14] P. 3, lines 15-17.

network, polices applicable to only a subset of the computing devices, and/or polices applicable to an individual computing device within the network.[15]

The invention of claim 1 is directed to a method for automatically provisioning a plurality of computing devices in accordance with established policies. A plurality of templates reflecting the policies is created.[16] At least one template is expanded at a central location to create a document comprising expanded information.[17] The document comprising the expanded information is sent from the central location to the plurality of computing devices.[18]

The invention of claim 8 is directed to a system for automatically provisioning a plurality of computing devices in accordance with established policies. The system includes a database system 32, a plurality of agents 36, and a communications gateway 38.[19] The database system 32 stores a plurality of templates which reflect the policies.[20] At least one of the templates is configured to selectably incorporate a policy defined only by a different template.[21] The agents 36 are respectively resident on each of the plurality of computing devices, and communicate with the database system to obtain information with regard to provisioning and maintenance of the respective computing devices.[22] Communication messages are exchanged between the agents 36 and the database system 32 through the communications gateway 38.[23] The communications gateway 38 is configured to: retrieve individual ones

---

[15] P. 3, lines 17-19.

[16] Fig. 4a, 402, 204, 406; P. 9, lines 21-27.

[17] Fig. 4a, 408, 410, 412; P. 9, line 28 to P. 10, line 5.

[18] Fig. 4a, 414, 416; P. 10, lines 4-5.

[19] Fig. 3; P. 5, line 26 to P. 6, line 4; P. 6, lines 21-23.

[20] P. 6, lines 8-9; P. 7, lines 1-4.

[21] P. 7 line 22 to P. 8 line 6.

[22] P. 5, lines 1-3.

[23] P. 6, lines 23-27.

of the plurality of templates; expand the retrieved templates to create respective documents containing combined template information and expanded information; and provide the documents containing the combined template information and expanded information to the plurality of agents 36.[24]

The invention of claim 22 is directed to a method of controlling user access to networked computing devices. A plurality of templates that identify user-access policies for respective ones of said devices is stored.[25] At least one of the templates includes a reference to information that is external to the template.[26] Further, at least one of the templates is configured to selectably incorporate a policy defined only by a different template.[27] A template that pertains to a given one of the devices is retrieved, and a document comprising a listing of users identified in the template and users identified by any externally referenced information is created at a central location 38.[28] The document is sent from the central location 38 to the given one of the devices.[29]

The invention of claim 31 is directed to a method for controlling user access to networked computing devices. A plurality of templates that identify user-access policies for respective ones of the devices is stored.[30] At least one of the templates includes a conditional statement.[31] A template that pertains to a given one of the devices is retrieved, and a document comprising a listing of users identified in the template, and users identified in any conditional statement

---

[24]P. 6, lines 23-27; P. 10, lines 1-4; P. 10, line 4-5.

[25] P. 7, lines 1-4. P. 6, lines 4-6.

[26] P. 8, lines 8-10.

[27] P. 7 line 22 to P. 8 line 6.

[28] Fig. 4, 408-414; P. 8, lines 29-33; P. 9, line 28 to P. 10, line 4; P. 6, lines 23-27.

[29] Fig. 4 416; P. 10, lines 4-5.

[30] P. 7, lines 1-4; P. 6, lines 4-6.

[31] P. 8, lines 8-11.

if said given device meets the condition, is created at a central location 38.[32] The document is sent from the central location 38 to the given one of the devices.[33] At least one of the templates is configured to selectably incorporate a policy defined only by a different template.[34]

[32] Fig. 4, 408-414; P. 9, line 28 to P. 10, line 4; P. 9, lines 3-20; P. 6, lines 23-27.

[33] Fig. 4 416; P. 10, lines 4-5.

[34] P. 7 line 22 to P. 8 line 6.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4-6, 8, 10-12, 39 and 41 are anticipated under 35 U.S.C. § 102(e) by Bonn et al. (U.S. Pat. No. 6,738,908, hereinafter "*Bonn*").

Whether claims 3, 7, 9, 13, 16, 17, 20-22, 24-31 and 33-36 are obvious under 35 U.S.C. § 103(a) over *Bonn* in view of Rothermel (U.S. Pat. No. 6,678,827, hereinafter "*Rothermel*").

Whether claims 37, 38, 40 and 42 are obvious under 35 U.S.C. § 103(a) over *Bonn* and *Rothermel* in view of Teng et al. (U.S. Pat. No. 7,380,008, hereinafter "*Teng*").

VII. ARGUMENT

A. Rejections under 35 U.S.C. § 102(e) over *Bonn*

1. Independent Claim 1

Independent claim 1 requires "expanding at least one template at a central location to create a document comprising expanded information; and sending from the central location the document comprising the expanded information to said plurality of computing devices." The Examiner cited *Bonn* col. 6, lines 30-53, Fig. 1A, and col. 4, lines 38-51 as allegedly teaching "sending … the document … to said plurality of computing devices."

Bonn col. 6, lines 30-53 describe Fig. 5 and teach steps for generating and implementing network security policies for a number of networks. For each network, a security policy is generated by mapping network elements to the aliases of a generalized template applicable to all the networks.[35] The security policy is transmitted to the network security device for the network.[36] In *Bonn*, each network is protected by a security device 200 as shown in Fig. 2.

Bonn col. 4, lines 38-51 describe Fig. 1A and teach generation of security policies for several networks from a single template in a manner duplicative of that described in *Bonn* col. 6, lines 30-53.

Thus, *Bonn* teaches that for each network a unique security policy is generated and sent to the security device corresponding to a network. *Bonn* teaches that the policy is sent only to this single device rather than to a "plurality of computing devices" as required by claim 1. The difference is significant because whereas *Bonn* teaches that each network is protected by a single security device that regulates access to the devices on the network, and a unique security policy is transmitted to each security device, claim 1 requires that each of the devices is configured according to a single document generated by expanding a template.

---

[35] *Bonn*, col. 6, lines 38-47.

[36] *Bonn*, col. 6, lines 47-50.

Bonn teaches using "the profile for the network to replace occurrences of aliases in the template with the addresses of the corresponding specific network elements ... [and sending] the resulting network specific policy to the network security device of the network for implementation."[37] Building a network specific policy as taught by *Bonn* and sending the policy to security devices other than the single security device protecting the network is contrary to *Bonn* because the policy was not built constructed based on those other networks. Consequently, the policy is non-functional or detrimental with regard to other networks as the security devices for those networks attempt to implement a policy which is based on addresses for a different network.

"For a prior art reference to anticipate in terms of 35 U.S.C. § 102, every element of the claimed invention must be identically shown in a single reference."[38] For at least the reason given above, Appellant respectfully submits that *Bonn* fails to identically show every element of claim 1, and therefore, the Examiner erred in rejecting claims 1-2, 4-6, and 39.

2. Claims 4-6

The Examiner rejected claims 4-6 as allegedly anticipated by *Bonn*. However, claims 4-6 depend from and incorporate all the limitations of claim 3. The Examiner admitted that *Bonn* fails to teach all the limitations of claim 3.[39] Therefore, Appellant respectfully submits that the Examiner erred in rejecting claims 4-6 under 35 U.S.C. § 102 over *Bonn*.

3. Independent Claim 8

Independent claim 8 requires "a database system which stores a plurality of templates which reflect said policies." The Examiner cited *Bonn* col. 6, lines 25 as allegedly teaching these limitations. The cited portion of *Bonn* teaches a memory that contains policy templates. However, no one skilled in the computer arts would equate a memory or a computer system comprising

---

[37] *Bonn*, col. 2, lines 25-29.

[38] *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990).

[39] *Final Office Action*, pp. 6-7 (Oct. 27, 2010).

memory with a database system. According to the Microsoft Computer Dictionary 5th Ed. (2002), a *database* is a file composed of records, each containing fields together with a set of operations for searching, sorting, recombining, and other functions." *Bonn* fails to teach any such structure, and fails to even mention a *database*.

Claim 8 also requires that "at least one of the templates are configured to selectably incorporate a policy defined only by a different template." The Examiner cited *Bonn* col. 8, lines 38-54 as allegedly teaching these limitations. *Bonn* col. 8, lines 38-54 teaches that a template can be used to generate policies, and principally teaches the display of Fig. 16 listing several different templates, where each template preferably corresponds to a different set of security services. Each listed template is generated using a process including: naming, adding rules, modifying rules, and adding aliases.[40] None of the template creation steps of *Bonn*, col. 6, line 57 to col. 8, line 37 teach a template "configured to selectably incorporate a policy defined only by a different template." *Bonn* col. 8, lines 38-54 is similarly deficient in that it teaches only the existence of templates corresponding to different services, but fails to teach a template "configured to selectably incorporate a policy defined only by a different template." Appellant is unable to identify any relationship between the templates described by *Bonn* and indicating that a template is configured to incorporate a policy defined by another template or to selectively incorporate such a policy. Rather, the *Bonn* templates appear to be distinct entities that are fully self-defined, with the exception profile mapping which does not involve incorporation from a different template.[41]

For at least these reasons, Appellant respectfully submits that *Bonn* fails to identically show every element of claim 8, and therefore, the Examiner erred in rejecting claims 8, 10-12, and 41 over *Bonn*.

---

[40] *Bonn*, col. 6, line 57 to col. 8, line 37.

[41] *Bonn*, col. 6, lines 30-52.

4. Claims 10-12

The Examiner rejected claims 10-12 as allegedly anticipated by *Bonn*. However, claims 4-6 depend from and incorporate all the limitations of claim 9. The Examiner admitted that *Bonn* fails to teach all the limitations of claim 3.[42] Therefore, Appellant respectfully submits that the Examiner erred in rejecting claims 10-12 under 35 U.S.C. § 102 over *Bonn*.

B. Rejections under 35 U.S.C. § 103(a) over *Bonn* and *Rothermel*

1. Independent Claim 22

Independent claim 22 requires "creating a document at a central location comprising a listing of users identified in said template and users identified by any externally referenced information." The Examiner admitted that *Bonn* fails to teach these limitations,[43] and cited *Rothermel*, col. 11, lines 18-30 as allegedly so teaching. The cited portion of *Rothermel* refers to *Rothermel* Fig. 3F, an example of a user interface for configuring a security policy template showing a "ping" service and a "Watchguard" service. The cited portion of *Rothermel* further teaches that configuring a network security device can include specifying customer contact information. However, *Rothermel* does not teach or suggest that the expanded template includes a "listing of users identified in said template." "Company name, contact person, customer ID, etc." is not a listing of users, but rather information usable to contact a purchaser of an NSD. Moreover, the cited portion of *Rothermel* fails to teach or suggest that customer contact information is included in the document created via template expansion.

Furthermore, the cited portion of *Rothermel* fails to teach or suggest that the document created via template expansion includes *users identified by externally referenced information*. The cited portion of *Rothermel* fails to even mention including externally referenced users lists in template expansion.

---

[42] *Final Office Action*, pp. 6-7 (Oct. 27, 2010).

[43] *Final Office Action*, p. 9 (Oct. 27, 2010).

Claim 22 also requires that "configuring at least one of the templates to selectably incorporate a policy defined only by a different template." The Examiner cited *Bonn* col. 8, lines 38-54 as allegedly teaching these limitations. The limitations are similar to limitations of claim 8 discussed above. As explained with regard to claim 8, *Bonn* fails to teach or suggest these limitations. *Rothermel* fails to satisfy this deficiency of *Bonn*.

For at least these reasons, Appellant respectfully submits that *Bonn* and *Rothermel* fail to teach or suggest the limitations of claim 22, and the Examiner has failed to state a prima facie case of obviousness with regard to claim 22. Therefore Appellant respectfully submits that the Examiner erred in rejecting independent claim 22 and claims 24-30 depending from claim 22.

2. Independent Claim 31

Independent claim 31 requires "retrieving a template that pertains to a given one of said devices and creating a document at a central location comprising a listing of users identified in said template, and users identified in any conditional statement if said given device meets the condition; ... and configuring at least one of the templates to selectably incorporate a policy defined only by a different template." These limitations are similar to those of claim 22 discussed above. As explained with regard to claim 22, *Bonn* and *Rothermel* fail to teach or suggest these limitations. Therefore, Appellant respectfully submits that the Examiner erred in rejecting independent claim 31 and claims 33-36 depending from claim 31 for much the same reasons as are given above with regard to claim 22.

3. Claims 3, 7, 9, 13, 16-17, and 20-21

Claims 3, 7, 20, and 21 depend from independent claim 1. Claims 9, 13, 16, and 17 depend from independent claim 8. *Rothermel* fails to satisfy the deficiencies of *Bonn* discussed above with regard to claim 1 and claim 8. Therefore, Appellant respectfully submits that claims 3, 7, 20, and 21 are allowable over *Bonn* and *Rothermel* for much the same reasons as are given above with regard to claim 1. Appellant further submits that claims 9, 13, 16,

and 17 are allowable over *Bonn* and *Rothermel* for much the same reasons as are given above with regard to claim 8.

a) Claims 3 and 9

Claims 3 and 9 are allowable for an additional reason. Claims 3 and 9 require that the "plurality of templates include[] conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided." The Examiner admitted that *Bonn* fails to teach these limitations, and cited *Rothermel* col. 10, lines 25-35, Fig. 3B, and Fig.8 as so allegedly teaching.[44] Fig. 3B and related text at col. 10, lines 25-35 teach security policy creation by application of the alias "Information Services." *Rothermel* teaches that "[i]n general, a network profile contains an alias definition like alias definition 311 for each alias used in the security policy template."[45] "[F]or each . . . rule in security policy template 300, each occurrence of an alias is replaced with the network addresses of the network elements defined to be within the alias in the network profile 310."[46] Thus, *Rothermel* teaches that the template is expanded based on the network profile 310, but fails to teach that rule 301 includes a conditional statement that determines whether the template is to be expanded.

Fig. 8 is a flow diagram of a subroutine 720 that determines whether network packets match one or more security policy filter rules.[47] Thus, Fig. 8 teaches application of security policy rather than conditional template expansion.

For at least these additional reasons, Appellant respectfully submits that *Bonn* and *Rothermel* fail to teach or suggest the limitations of claims 3 and 9, and respectfully submit that the Examiner erred in rejecting claims 3 and 9, and all claims respectively depending from therefrom.

---

[44] *Final Office Action*, pp. 6-7 (Oct. 27, 2010).

[45] *Rothermel*, col. 10, lines 44-46.

[46] *Rothermel*, col. 10, lines 56-59.

[47] *Rothermel*, col. 15, lines 30-33.

4. Claim 24

Claim 24 requires that "said external information comprises a list of users." The Examiner admitted that *Bonn* fails to teach these limitations, and cited *Rothermel*, col. 11, lines 18-30 as allegedly so teaching.[48] The cited portion of *Rothermel* teaches including customer contact information in a security policy.[49] Claim 24 recites "a method of controlling user access." The "users" of claim 24 are therefore those whose access is controlled. *Rothermel* fails to teach that the customer contact is a "user" of the computing device to which the template applies to "control user access," but rather simply a contact person with the customer entity. For at least this additional reason, Appellant respectfully submits that the Examiner erred in rejecting claims 24-25.

5. Claims 28 and 34

Claims 28 and 34 require "a template in said second category inherits policies contained in a template of said first category." The Examiner cited *Bonn* col. 8, lines 42-54 as allegedly teaching these limitations. The cited portion of *Bonn* teaches different templates each corresponding to a different set of security services and each individually generated by the steps shown in Figs. 6-15. *Bonn* fails to teach or suggest that any template inherits policies contained in a template of different category, but rather teaches that each template is created by adding and amending rules with no mention or description whatsoever of inheritance. *Rothermel* fails to satisfy this deficiency of *Bonn*. For at least these additional reasons, Appellant respectfully submits that the Examiner erred in rejecting claims 28-30 and 34-36.

6. Claims 29 and 35

Claims 29 and 35 require that "inheritance can be selectively disabled." The Examiner cited *Bonn* col. 9, lines 1-20 as allegedly teaching these limitations. *Bonn* col. 9, lines 1-20 teach generating a network profile for new network. The network profile is mapped to a template to generate network

[48] *Final Office Action*, p. 9 (Oct. 27, 2010).

[49] *Rothermel*, col. 11, lines 24-26.

security policies for the new network,[50] but generation of a network profile is not and does not suggest template to template inheritance or that inheritance can be selectively disabled as required by claims 29 and 30. Instead the network profile defines that values that will mapped into the template. *Rothermel* fails to satisfy this deficiency of *Bonn*. For at least these additional reasons, Appellant respectfully submits that the Examiner erred in rejecting claims 29 and 35.

C. Rejections under 35 U.S.C. § 103(a) over *Bonn* and *Rothermel* and *Teng*

Claims 37, 38, 40, and 42 depend from claims 31, 22, 1, and 8 respectively. *Teng* fails to satisfy the deficiencies of *Bonn* and *Rothermel* explained above with regard to claims 31, 22, 1, and 8. Therefore, Appellant respectfully submits that claims 37, 38, 40, and 42 are allowable over the cited art for much the same reasons as are given above with regard to the independent claims from which each respectively depends.

D. Conclusion

For the reasons stated above, Appellant respectfully submits that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/David M. Wilson/

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528

David M. Wilson, PTO Reg. No. 56,790
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANT

[50] *Bonn*, col. 6, lines 30-52.

VIII. CLAIMS APPENDIX

1. A method for automatically provisioning a plurality of computing devices in accordance with established policies, the method comprising the steps of:

creating a plurality of templates reflecting said policies;

expanding at least one template at a central location to create a document comprising expanded information; and

sending from the central location the document comprising the expanded information to said plurality of computing devices.

2. The method of claim 1, further comprising interpreting the expanded information by agents which are respectively resident on each of said plurality of computing devices.

3. The method of claim 1, wherein the structure of said plurality of templates includes conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided.

4. The method of claim 3, wherein the plurality of templates includes a first category of templates that reflect policies applicable to all of the plurality of computing devices.

5. The method of claim 4, wherein the plurality of templates includes a second category of templates that reflect policies applicable to only a subset of the plurality of computing devices.

6. The method of claim 4, wherein the plurality of templates includes another category of templates that reflect policies applicable to only a particular type of the plurality of computing devices.

7. The method of claim 1, wherein said policies are security polices regarding user access to each of the plurality of computing devices.

8. A system for automatically provisioning a plurality of computing devices in accordance with established policies, the system comprising:

a database system which stores a plurality of templates which reflect said polices;

a plurality of agents which are respectively resident on each of said plurality of computing devices, and which communicate with said database system to obtain information with regard to provisioning and maintenance of the respective computing devices; and

a communications gateway through which communication messages are exchanged between said agents and said database system, wherein said communications gateway is configured to:

retrieve individual ones of the plurality of templates;

expand the retrieved templates to create respective documents containing combined template information and expanded information; and

provide the documents containing the combined template information and expanded information to said plurality of agents;

wherein at least one of the templates are configured to selectably incorporate a policy defined only by a different template.

9. The system of claim 8, wherein the structure of said plurality of templates includes conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided.

10. The system of claim 9, wherein the plurality of templates includes a first category of templates that reflect policies applicable to all of the plurality of computing devices.

11. The system of claim 10, wherein the plurality of templates includes a second category of templates that reflect policies applicable to a subset of the plurality of computing devices.

12. The system of claim 10, wherein the plurality of templates includes another category of templates that reflect policies applicable to a particular type of the plurality of computing devices.

13. The system of claim 8, wherein said policies are security polices regarding user access to each of the plurality of computing devices.

16. The system of claim 41 wherein said external information comprises a list of users.

17. The system of claim 9 wherein said communications gateway expands a template to include information contained in a conditional statement only if the computing device to which said expanded information is to be provided meets the condition.

20. The method of claim 39, wherein said external information comprises a list of users.

21. The method of claim 3, wherein said expanding step includes the step of including information contained in a conditional statement only if the computing device to which said expanded information is to be provided meets the condition.

22. A method of controlling user access to networked computing devices, comprising the steps of:

storing a plurality of templates that identify user-access policies for respective ones of said devices, at least one of said templates including a reference to information that is external to the template;

retrieving a template that pertains to a given one of said devices and creating a document at a central location comprising a listing of users identified in said template and users identified by any externally referenced information; and

sending said document from said central location to the given one of said devices;

configuring at least one of the templates to selectably incorporate a policy defined only by a different template.

24. The method of claim 22 wherein said external information comprises a list of users.

25. The method of claim 24 wherein all of the users on said list perform a specified role relative to said computing devices.

26. The method of claim 22 wherein at least one of said templates includes a conditional statement, and the step of creating a document comprises including

information from said conditional statement in said document only if said given device meets the condition.

27. The method of claim 22, wherein said plurality of templates are classified into at least two categories, wherein a template in a first category pertains to all of the computing devices, and a template in a second category pertains to a subset of said computing devices.

28. The method of claim 27, wherein a template in said second category inherits policies contained in a template of said first category.

29. The method of claim 28, wherein said inheritance can be selectively disabled.

30. The method of claim 28, further including a third category of templates that pertain to specific devices and inherit policies from templates in said second category.

31. A method for controlling user access to networked computing devices, comprising the steps of:

storing a plurality of templates that identify user-access policies for respective ones of said devices, at least one of said templates including a conditional statement;

retrieving a template that pertains to a given one of said devices and creating a document at a central location comprising a listing of users identified in said template, and users identified in any conditional statement if said given device meets the condition; and

sending said document from said central location to the given one of said devices;

configuring at least one of the templates to selectably incorporate a policy defined only by a different template.

33. The method of claim 31, wherein said plurality of templates are classified into at least two categories, wherein a template in a first category pertains to all of the computing devices, and a template in a second category pertains to a subset of said computing devices.

34. The method of claim 33, wherein a template in said second category inherits policies contained in a template of said first category.

35. The method of claim 34, wherein said inheritance can be selectively disabled.

36. The method of claim 34, further including a third category of templates that pertain to specific devices and inherit policies from templates in said second category.

37. The method of claim 31, wherein said document is an XML document.

38. The method of claim 22, wherein said document is an XML document.

39. The method of claim 1, wherein at least one template includes a reference to information external to the template, and wherein said expanding step comprises creating the document that includes information contained in the template and said external information.

40. The method of claim 39, wherein said document is an XML document.

41. The system of claim 8, wherein at least one template includes a reference to information external to the template, and wherein said communication gateway expands the template by creating a document that includes information contained in the template and said external information.

42. The system of claim 41 wherein said document is an XML document.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.